AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with a certain wireless number assigned IPV6 **2600:0001:9313:1304:3448:d9cf:5dca:99a9** utilized 2018-08-16 16:31:56 UTC ("the SUBJECT PHONE"), more fully described in **Attachment A.**

Case No. 18-M-134 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Information associated with a certain wireless number assigned IPV6 **2600:0001:9313:1304:3448:d9cf:5dca:99a9** utilized 2018-08-16 16:31:56 UTC ("the SUBJECT PHONE"), more fully described in **Attachment A**

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See **Attachment B.**

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, § 3148 (Violations of the conditions of release pending sentencing)

The application is based on these facts: See attached affidavit.

☒ Delayed notice of 30 days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Scott Keller, Deputy U.S. Marshal

Printed Name and Title

Sworn to before me and signed in my presence:

Date: Aug 17, 2018 4:53 p.m.

Judge's signature

City and State: Milwaukee, Wisconsin

Honorable David E. Jones, U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Scott Keller, being duly sworn, depose and state as follows:

BACKGROUND AND EXPERIENCE

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned IP Address **2600:0001:9313:1304:3448:d9cf:5dca:99a9**, utilized 2018-08-16 16:31:56 UTC ("the SUBJECT PHONE") that is stored at premises controlled by **Sprint**, a wireless telephone service provider headquartered at 6480 **Sprint** Parkway, Overland Park, KS 66251. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require **Sprint** to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B

2. I am a Deputy with the U.S. Marshals Service, and have been since May 2010. As part of my duties, I investigate violations of federal and state laws, including those relating to fugitives. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

3. This affidavit is based upon my personal knowledge and information reported to me by other federal, state, and local law enforcement officers during the course of their official

duties, all of whom I believe to be truthful and reliable. This affidavit concerns a fugitive investigation taking place in the Eastern District of Wisconsin. The target of the investigation is Marquille D. Wimberly.

4. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that that the information described in Attachment B will assist law enforcement in locating and arresting Wimberly, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

SOURCES OF INFORMATION

6. I have obtained the facts set forth in this affidavit through my personal participation in the investigation described below; from oral and written reports of other law enforcement officers participating in this and related investigations, and from records, documents and other evidence obtained during this investigation. Since this affidavit is being submitted for the limited purpose of obtaining call detail records, along with cell site and GPS data, I have not included every fact known concerning this investigation. I have set forth only the facts that I believe are essential to establish the necessary foundation for an order authorizing call detail records, along with cell site and GPS data.

PROBABLE CAUSE

7. The United States government, including the USMS, is investigating violations of Title 18, United States Code, Section 3148 committed by Marquille D. Wimberly.

8. On August 1, 2017, Wimberly was indicted in the Eastern District of Wisconsin (Case No. 17-CR-134) for unlawfully possessing a firearm and ammunition as a convicted felon, in violation of Title 18, United States Code, Sections 922(g)(1), 922(g)(9), and 924(a)(2).

9. On October 3, 2017, an order setting conditions of release for Wimberly was signed by a federal judge. Among the conditions of his release, Wimberly was required to wear an electronic monitoring ankle bracelet, that he be placed on home detention at his mother's residence, and that he not violate federal, state, or local laws.

10. On May 28, 2018, the Milwaukee Police Department was dispatched to St. Luke's Hospital in Milwaukee. A female victim reported to police that Wimberly had hit her in the face with a closed fist breaking her jaw and chipping her tooth. Milwaukee Police Department officers went to the residence where the assault occurred to speak with Wimberly. Wimberly was not there at the time. Wimberly's mother gave consent for the officers to take pictures of the bathroom the victim used to clean the blood off her face. Photos of blood splattered on the wall were taken.

11. On May 28, 2018, Wimberly cut off the electronic monitoring ankle bracelet and absconded from pre-trial supervision.

12. On May 30, 2018, a federal arrest warrant was issued for Wimberly based on his suspected violation of the conditions of his pre-trial release.

13. On June 4, 2018, a state arrest warrant was issued for Wimberly based on his alleged assault of the female victim described above.

14. On July 15, 2018, a 25-year old male victim was approached on a street in Milwaukee and shot six times. A female observed the male victim lying on the ground and

transported him to the hospital. The victim identified Wimberly as the shooter. The investigation into this incident is ongoing.

15. On July 25, 2018, the female witness who transported the above mentioned male victim was shot and killed. A temporary felony arrest warrant for homicide was issued for Wimberly by the Milwaukee Police Department.

16. On July 25, 2018, I conducted an open records search of Facebook using Marquille Wimberly as a search term. As a result, I was able to identify an account associated with Wimberly.

17. I observed photos which I believe to be Wimberly after comparing Facebook photos to Wimberly's known Wisconsin Department of Transportation photo and Eastern District of Wisconsin mugshot.

18. Wimberly regularly posts publicly on his Facebook page. On July 30, 2018, Wimberly made a public post of himself with his son and comments.

19. On August 1, 2018, I served Facebook with a preservation request pursuant to 18 U.S.C. § 2703(f), requiring Facebook to preserve all information associated with the account associated with Wimberly.

20. On August 2, 2018, United States Magistrate Judge David Jones in the Eastern District of Wisconsin, authorized a Pen register Trap and Trace order for Wimberly's Facebook account, https://www.facebook.com/mark.moeta, Facebook ID number 100013982976380. On that same date, Facebook was served with the legal demand.

21. Information related to the Pen register Trap and Trace order became available on August 3, 2018. The information obtained showed that the Internet Protocol (IP) addresses

utilized most frequently to access the Facebook account associated with Wimberly were assigned to the Internet Service Provider (ISP) **Sprint**.

22. Based on training and experience, I know that **Sprint** is a cellular service provider and does have the ability to connect their cellular service to the internet through Dynamic Internet Protocols. A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network. A dynamic IP address is an automatically configured IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server to every new network node.

23. Dynamic IP addresses are generally implemented by Internet service providers and networks that have a large number of connecting clients or end-nodes. Unlike static IP addresses, dynamic IP addresses are not permanent. A dynamic IP is assigned to a node until it's connected to the network; therefore, the same node may have a different IP address every time it reconnects with the network.

24. On August 5, 2018, Wimberly posted a photo publicly on his Facebook page, https://www.facebook.com/mark.moeta, Facebook ID number 100013982976380. The profile name on this account is Maquille D. Wimberly. The photo appears to be taken by Wimberly, as it shows himself in the front passenger seat of a vehicle, and also shows an associate in the driver's seat and two more associates in the rear seats of the vehicle. This photo was compared to Wimberly's WI DOT photo and found to be the same person. Wimberly is clearly in the forefront and the others are in the background. Minutes prior to that photo being posted, the pen register data showed that Wimberly was utilizing a **Sprint** device to access his account.

25. Because the activity on his Facebook account showed consistent use of a **Sprint** device, as well as the identifying use of a **Sprint** device at the same time Wimberly posted a publicly visible photo of himself, it was believed that Wimberly was in possession of a **Sprint** device. Based on this information, a request for a search warrant for historical data and GPS data was submitted.

26. On August 6, 2018, Milwaukee Police officers observed Wimberly at a location he was known to frequent on the north side of Milwaukee. As officers attempted to apprehend Wimberly, he got in a nearby by vehicle and fled. Officers gave chase, but Wimberly was able to avoid arrest. The vehicle was later discovered parked on the side of the road miles away from the location where the pursuit began.

27. On August 7, 2018, United States Magistrate Judge David Jones in the Eastern District of Wisconsin authorized a search warrant for historical call detail records and real time GPS associated with the **Sprint** IPV6 identified through the Facebook Pen Register Trap and Trace.

28. Records later received from **Sprint** revealed that Wimberly likely possessed the initial **Sprint** phone until approximately August 6, 2018. In particular, the records show that the location of the device mirrors the route taken during the chase and also shows a consistent location as to where the vehicle was later located. Following the August 6, 2018, vehicle pursuit, the call patterns appeared to change.

29. Following the August 6, 2018 vehicle pursuit, Wimberly's Facebook activity decreased for a couple of days. When Wimberly's Facebook account was next utilized, it was from an IP addresses associated with a T-Mobile device.

30. On August 10, 2018, United States Magistrate Judge David Jones in the Eastern District of Wisconsin authorized a search warrant for historical call detail records and real time GPS associated with the T-Mobile device.

31. Further investigation identified a current address associated with the subscriber of the T-Mobile device in East St. Louis, Illinois.

32. On August 16, 2018, United States Fugitive Task Force members in East St. Louis contacted a woman living at the address associated with the T-Mobile device. The woman told Task Force officers that she is Wimberly's cousin and Wimberly had been staying with her from approximately August 7th to approximately August 14th or 15th. According to the woman, Wimberly showed up at her residence the prior week and asked to stay with her for a few days. While at the residence, Wimberly used the woman's phone on occasion. Task force members were able to confirm the number for cousin's T-Mobile device is the same number identified as being utilized by Wimberly. The cousin was unable to provide any further information concerning Wimberly's present whereabouts or any individual(s) with whom Wimberly may be traveling or staying.

33. That same day, August 16, 2018, an individual, believed to be Wimberly, utilized Wimberly's Facebook account. According to the pen register trap and trace associated with the Facebook account, the person utilized the account from IPV6 address **2600:0001:9313:1304:3448:d9cf:5dca:99a9** on 2018-08-16 at 16:31:56 UTC (Coordinated Universal Time) and the person utilizing the account was identified as the accountholder, who is Marquille D. Wimberly. A check of the American Registry for Internet Number (ARIN), the ISP assigned this IPV6 address is **Sprint**.

34. Based on the foregoing, records and location information associated with the Sprint device assigned IP Address **2600:0001:9313:1304:3448:d9cf:5dca:99a9**, utilized 2018-08-16 16:31:56 UTC, that would be developed through historical records and cell site data will be useful and important in attempting to locate and apprehend Wimberly. These records include records of the usage of the device prior to the time Wimberly is believed to have initially used the device in order to identify any changes in the pattern of usage and thereby attempt to verify Wimberly's current use of the device.

35. I know through training and experience, that **Sprint** is able to resolve IPV6 addresses. When **Sprint** resolves those IP addresses, they are able to identify the user and the specific cellular phone associated with that user. Therefore, providing **Sprint** with the IP address and time stamp, is the same as providing **Sprint** with the target cellular number. The identified IP address and time stamp of, IPV6 Address **2600:0001:9313:1304:3448:d9cf:5dca:99a9**, utilized on 2018-08-16 at 16:31:56 UTC, will take the place of the cellular number, referred to as the "Target Number."

36. In my training and experience, I have learned that **Sprint** is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart,

even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

37. Based on my training and experience, I know that **Sprint** can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as **Sprint** typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

38. Based on my training and experience, I know that wireless providers such as **Sprint** typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as **Sprint** typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONE's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

39. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

40. I further request that the Court direct **Sprint** to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on **Sprint**, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

41. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned IP address **2600:0001:9313:1304:3448:d9cf:5dca:99a9**, utilized 2018-08-16 16:31:56 UTC ("the Account"), that are stored at premises controlled by **Sprint** ("the Provider"), headquartered at 6480 **Sprint** Parkway, Overland Park, KS 66251.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period **July 17, 2018 to present.**

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 3148 involving Marquille D. Wimberly since May 1, 2018.